Technical Cybersecurity

Evolution

'70-'75: Technical Interest

STARTED WITH TECHIES PLAYING AROUND

‣ Early programs and systems had NO SECURITY

‣ Early malware and hacking were for fun, pranks

‣ Small groups of people, essentially non-criminal

'70-'80: Becoming Darker

Malware started to cause problems

‣ Some were mischievous, printing messages, taunting

‣ …others were not

See malware techniques in open

‣ Some are creating malware as primitive DRM

‣ …too bad Sony wasn't paying attention

Malicious, evolving

‣ New techniques: polymorphic, multipartite, etc.

‣ Deliberate system destruction

’80-’90: Greed

No real criminal organizations yet

‣ …but definite criminal intention

The law is paying attention

‣ …but they are too draconian

‣ New legislation submitted, soon to pass

'90-'00: Arrests & Gov't

GOVERNMENT HACKS & MORE CRIME

- ‣ Online defacement
- ‣ US Military hacks
- ‣ Millions stolen from banks

SECURITY GETS SERIOUS

- ‣ Vendors start releasing patches more quickly
- ‣ Developers start paying attention

'00-now: Deadly Serious

RANSOMWARE

‣ Surprisingly unprofitable

NATION-STATES

‣ APT groups

ORGANIZED CRIME

‣ Serious money, serious criminals

MAAS

‣ Malware-as-a-service

How does this effect IoT?